21st TSC Security Manager's Guide

Purpose

- This class describes some of the basic security procedures that you should be aware of if you are responsible for security manager duties. The procedures described within are not all encompassing. We have included only those that are commonly associated with being a security manager in the 21st Theater Support Command. Be sure to contact your security office for more detailed information on these and other pertinent procedures. Use this class as an introduction to security or as a security refresher/reminder.

Layout

- The basic information has been taken from *The Layman's Guide to Security*, dated March 1997, published by the Department of Defense Security Institute and augmented by USAREUR Security Branch (see "contents" below) The information has been divided into sections based on functional areas performed by a security manager. Within these sections, the more likely security procedures or concerns are described. If your job dictates duties other than those described, check with the Command Security Manager or look at the "index" to see if those other procedures are described in another section. Hyperlinks have been added to enable you to advance to your section.

Contents

- Security Manager
- Classification Management
- Personnel Security
- Information Systems Monitoring
- Information Systems Security
- SAEDA
- OPSEC
- Travel Policy
- Foreign Nationals access to USAREUR Installations
- Oversight Staff Evaluations
- Index

Security Manager

- AR 380-5, 25 Feb 88
- UR Suppl 1 to AR 380-5, 18 Jul 89

Back to Table of Contents

Index

Security Manager

- Commanders will appoint security managers in writing for unit down to and including company level
- Unit and agency security managers will administer the security program

Back to Table of Contents

Index

Who Can Be a Security Manager?

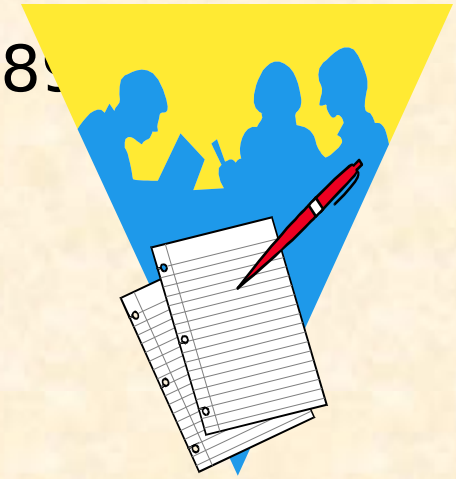
- The minimum rank requirement for USAREUR Security Managers for USAREUR major, separate, and assigned commands are Captain, GS-9, or above. For USAREUR Security Managers below the USAREUR major, separate, and assigned command level, the minimum rank requirements are Sergeant First Class, GS-7, or above.

Back to Table of Cont

Index

Classification Management

- AR 380-5, 25 Feb 88
- UR Suppl 1 to AR 380-5, 18 Jul 8
- Change 1, 28 Nov 89
- Change 2, 27 Jun 91
- Change 3, 17 Sep 92
- Change 4, 28 May 94
- Change 5, 21 Jul 95



Back to Table of Contents

Index

Accountability Systems

- Check with the security office for your activity's accountability for Top Secret, Secret, and Confidential materials
- Three book accountability, active, inactive, and destruction required for Top Secret and NATO Secret and above
- While accountability systems are not required for U.S. Secret or codeword materials, use of a DA 455 or any other simple register is recommended

Back to Table of Contents
Index

Procedures to Follow When Reproducing Classified Materials

- Use machines for which classified reproduction has been authorized and so designated
- Ensure latent images will not cause compromise
- Limitations and control procedures that apply to the originals must also be applied to the copies
- There is no authorization to copy NATO materials

Back to Table of Contents

Index

Procedures to Follow When Reproducing Classified Materials, (continued)

- Always check the copier to be sure that no classified originals or copies are left in it (print three blank copies before leaving)
- Place poor copies in an authorized container and destroy them as soon as possible
- Contractors: Obtain authorization from contracting activity for Top Secret unless contract requires reproduction. Keep record of reproduction Top Secret (2 years)

Back to Table of Contents

Index

Using Your Security Container

- Store all classified in locked container unless someone is present in the room who is authorized access
- Fill out SF 702 (security container check sheet) each time you:
  - Open
  - Close, or
  - Check

  the container.

Back to Table of Contents

Index

How to Mark Disks

- Use:
  - SF 706 (Top Secret label)
  - SF 707 (Secret label)
  - SF 708 (Confidential label)
  - SF 711 (data descriptor label)
  - To indicate highest level of classification contained on disk
- Place SF 710 (unclassified label) on unclassified disks that are stored with classified disks or used in an environment with classified materials
- Handle disks as if classified document

Back to Table of Contents

Index

What to Do With the Disk

- Place the proper classification label on the diskette
- Store the diskette in a proper security container when:
  - You leave the area and no authorized persons are there (if there is an authorized person around, tell them that the classified diskette is there.)
  - You are not using the diskette
- Keep materials in your possession
- Take it back to the distribution point and hand it to an authorized person or put it in an approved container, or
- Deliver it to the office at a later time and hand it to an authorized person
- Always have an individual sign for the classified document (use DA 3964)

Index **Back to Table of Contents**

How to Mark the Documents on Disks

- Mark portions electronically
- Apply interior page marking, overall document marking, and applicable associated marking (“derived from”, line, etc.) Electronically, if feasible; otherwise mechanically (either using stamps or a typewriter) place these markings on document after it is printed
- Ensure that the electronic marking is accurate for the information provided

Back to Table of Contents

Index

Minimum Marking Requirements for Paper Products

- First, mark all portions (paragraphs, drawing, caption, and subject/title lines) with highest level of classification (restrictive warning notices/caveats) found within that portion. Place marking at beginning of each portion (except subject/title lines which are marked after the portion) by using abbreviations and placing within parentheses

Back to Table of Contents

Index

Minimum Marking Requirements for Paper Products

- Second, conspicuously mark at the top and bottom of each interior page (all pages except title page, if any, and first page) the highest classification of information (and restrictive caveats, if any) contained on that particular page

Back to Table of Contents
Index

Minimum Marking Requirements for Paper Products

- Third, mark the top and bottom of:
  - The front cover, if any
  - The title page, if any
  - The first page, if any
  - The outside of the back cover, if any
  - With the highest level of classification of information contained within the document

Back to Table of Contents

Index

Minimum Marking Requirements for Paper Products

- Fourth, for a derivatively classified document, place on the front of the document the:
  - "Derived from" line
  - "Declassify on" line
  - Downgrading instructions, if any
  - Restrictive caveats, if any
  - Originating office and date
- (Check with your security office on how to mark an originally classified document)

Back to Table of Contents

Index

What to Do with Materials While Typing

- Do not leave the classified materials alone, if you must leave:
  - Ensure that an authorized person is there (tell individual about the materials), or
  - Lock the materials in an authorized security container
  - If in an unsecured area, ensure the typewriter ribbon is secured in an appropriate security container when not being used

Back to Table of Contents

Index

What to Do with the Typewriter/Printer Ribbon

- Indicate on the cartridge/cassette the classification level of the information on it. (One of the SF 706, 707, 708, 709, or 710 labels can accomplish this.) Properly destroy the cartridge/cassette as soon as feasible
- Store the cartridge/cassette in an approved security container when:
  - You leave the area and no authorized persons are there (if there is an authorized person around, be sure to tell the individual that the classified ribbon is there)
  - You are finished with your typing

Back to Table of Contents
Index

What to Do with the Drafts/Notes/etc

- Store the classified drafts/notes/etc in an authorized security container
- Give it to whoever wrote it or to someone with the appropriate clearance and need-to-know
- Drafts/notes are considered to be working papers and should be marked as such. After 90 days they become permanent documents. If they are NATO or Top Secret, there is a requirement to bring them under control

Back to Table of Contents

Index

Methods for Transmitting Classified Materials

- **Confidential:**
  - Authorized electronic system, e.g, a STU-III
  - Handcarry (with proper authorization)
  - Defense Courier Service (not routinely but under certain circumstances)
  - U.S. Postal Service registered mail to/from APO/FPO and Costa Rica
  - U.S. Postal Service first class mail inside the continental United States

Back to Table of Contents

Index

Methods for Transmitting Classified Materials

- **Confidential, continued:**

  - Registered mail (for APO/FPO outside U.S. and Puerto Rico: for NATO outside U.S.: when uncertain if destination within U.S.: to DoD contractor or other executive branch agency, when appropriate)

  - First class mail between DoD contractor or other executive branch agency in the U.S.

  - Constant surveillance service within U.S. boundaries if item is large and bulky (Check with MTMC for information on companies that provide this service)

Back to Table of Contents
Index

Methods for Transmitting Classified Materials

- **Secret:**
  - Authorization electronic system, e.g., a STU-III
  - Handcarrying (with proper authorization)
  - Defense courier service (not routinely but under certain circumstances)
  - Registered mail (within U.S. and Puerto Rico)
  - Registered mail to APO/FPO but only if mail will not pass out of U.S. control during entire mail process

Back to Table of Contents
Index

Methods for Transmitting Classified Materials

- **Secret, continued:**

  - Protective security service within U.S. boundaries if item is large and bulky (check with MTMC for information on the companies that provide this service)

  - U.S. Postal service express mail (within U.S. and Puerto Rico). Do not use to send to an APO/FPO address and do not use street-side collection box.

  - GSA contract holder for overnight delivery (currently FedEx) (within US and territories). See your security office for limitations and procedures. Do not send to an APO/FPO address.

Back to Table of Contents
Index

Methods for Transmitting Classified Materials

- **Top Secret:**
  - Defense courier service
  - Department of State courier service, only under rare conditions
  - Authorized electronic system, e.g. a STU-III
  - Handcarrying (with proper authorization)

Back to Table of Contents
Index

Using Distribution Systems

- Ensure classified materials are not left alone in distribution boxes
- Ensure only authorized personnel (with appropriate clearance and need-to-know) pick up classified materials

Back to Table of Contents
Index

Handling of Mail

- Protect mail until it has been determined whether or not classified materials are contained within
- For DoD contractors: ensure only cleared personnel receive and sign for all certified and registered mail

Back to Table of Contents
Index

What to Do When No One is in the Office to Receive Mail

- Keep materials in your possession
- Take it back to the distribution point and hand it to an authorized person or put it in an approved container, or
- Deliver it to the office at a later time and hand it to an authorized person
- Always have an individual sign for the classified document (use DA 3964)

Back to Table of Contents
Index

What to Do While Distributing Materials

- Keep materials in your personal possession at all times until you can hand it directly to someone else who has clearance and is authorized access to it
- Never leave classified material unattended while delivery is being made
- Ensure that it is signed for

Back to Table of Contents
Index

How to Prepare Classified Materials for Movement

- Double wrap (use opaque materials)
- Place classification marking on inner layer
- Do not indicate classification on outside layer
- Seal package in such a way that tampering can be detected
- Address package to an official address, not to a person

Back to Table of Contents
Index

Methods for Mailing Classified Materials

Top Secret:

- Mailing not authorized, use Defense Courier Service to transmit or
- Cleared and designated U.S. military and government civilian employees or
- If appropriate, the Department of State courier system (see AR 380-5, paragraph 8-101(a-i)

Back to Table of Contents
Index

Methods for Mailing Classified Documents (continued)

Secret:

- Registered mail within U.S. and Puerto Rico
- Registered mail to APO/FPO but only if mail will not pass out of U.S. control during the entire mail process
- Any means approved for transmission of Top Secret documents (see AR 380-5, paragraph 8-102)

Back to Table of Contents
Index

Methods for Mailing Classified Documents, (continued)

Confidential:

- U.S. Postal service registered mail to and from APO/FPO addresses located outside the U.S. and its Territories
- Means approved for transmission of Secret material
- U.S. Postal Service first class mail between DoD component locations anywhere in the U.S. and its Territories (see AR 380-5, paragraph 8-103)

Back to Table of Contents

Ind

Handcarrying

- Use handcarrying as your last means for transmitting classified materials. Use it only after all other transmission methods have been found inadequate
- Double wrap the materials
- Keep materials under constant surveillance and personal possession
- Do not place in detachable storage compartment, e.g. auto trailer, luggage rack, etc.
- Store overnight only at a U.S. government facility or cleared contractor facility with storage capability

Back to Table of Contents

Index

Handcarrying (continued)

- Leave a list (DA 3964) of materials being handcarried with your activity
- Get briefed prior to departure
- If using a commercial airline:
  - Coordinate with the airline before leaving
  - Have ID and letter of authorization
  - Allow x-raying but do not allow direct access to the information
  - Use U.S. flag carrier or allied flag carrier if U.S. is not available
- Check with your security office for more information on handcarrying

Back to Table of Contents
Index

Faxing Classified Information

- Use secure FAX unit
- Follow the encryption procedures for that piece of equipment
- Before transmitting, call the receiving office to ensure an authorized person is available to receive the transmission
- Remain with the unit until the transmission or reception is complete

Back to Table of Contents

Index

Transporting from Office to Office

- Do not attract attention to yourself when carrying classified materials from one office to another. Place the materials in a nondescript envelope or container
- Place cover sheet (SF 701, 704, or 705) on materials prior to placing into envelope to remind yourself and recipient that materials are classified

Back to Table of Contents

Index

Courier Orders

- Courier orders are required when you travel outside you assigned military area. The courier will be in possession of the appropriate courier authorization form as indicated below:

  - Travel within the country of assignment

  (use the DD form 2502, Courier Authorization Card)

  - Travel across international boundaries

  (use the AR 380-5E-R in English plus the appropriate German, Italian, Turkish or Greek, translation.)

  - Couriers of SCI

  (use USAREUR Form 32)

- Travel within your city of assignment does not require courier orders, except for SCI; however, you must have permission from your supervisor to transport classified material within your area.

Back to Table of Contents
Index

Who Can Destroy Classified Materials

- User (or custodian) of the materials
- Designated destruction official(s) for your activity, if used
- Witness required for the destruction of Top Secret and NATO Secret information

Back to Table of Contents
Index

What to Destroy

- Check with your records management office to identify those files that are considered “record files” and “historical files” for your office
- Destroy document if it’s a “non-record” document and no operational need for it
- Conduct annual clean-out day (identify documents no longer needed and destroy); review regularly during year as well
- Contractors: recommend you check with contracting agency prior to destruction

Back to Table of Contents
Index

How to Destroy Classified Materials

- Burning, (if allowed by your local environmental agency)
- Shredding (particle size must meet standard set by your component)
- Pulverizing (standards for equipment set by your component)
- Pulping (standards for equipment set by your component)
- Check with your security office for location of equipment and information on other methods

Back to Table of Contents

Index

Handling Classified Materials When They are Not in a Security Container

- Always ensure classified is under your direct control or that of someone who has appropriate clearance and is authorized access
- Put the appropriate clearance cover sheet (orange colored SF 703 for Top Secret; red SF 704 for Secret; blue SF 705 for Confidential) on the materials

Back to Table of Contents
Index

Using Your Security Container

- Store all classified in locked container unless someone is present in the room who is authorized access
- Fill out SF 702 (security container check sheet) each time you:
  - Open
  - Close, or
  - Check the container

Back to Table of Contents
Index

End of the Day Security Check

- Check the entire work area for classified materials
- Check the container to ensure it is locked
- Record this check on SF 701 (activity security checklist).
- Perform the above steps if you work with classified materials during non-working hours

Back to Table of Contents
Index

Who Can Have Access

- Only give access to classified material to people with appropriate clearance and a need-to-know

Back to Table of Contents
Index

Personnel Security

- AR 380-67, 9 Sep 88
- UR Suppl 1 to AR 380-67, 20 Jan 94
- DA Revised PSI and Adjudicative Standards, 22 Dec 98

Back to Table of Contents
Index

Security Clearance Investigative Requirements

- U.S. Military
  - Confidential & Secret: NACLC
  - Top Secret or Top Secret SCI: SSBI
- U.S. Civilian
  - Confidential & Secret: ANACI
  - Top Secret or Top Secret SCI: SSBI
- Military NACLC cannot be transferred to civilian position
  - ANACI is required (for suitability)
- SSBI may be transferred from military to civilian position after the ANACI is initiated.

Initial Investigations

- Go back 10 years on education, residence and employment
- All other information, go back 7 years

Back to Table of Contents
Index

Periodic Reinvestigations

- Confidential and Secret access: NACLC, local agency checks and credit check at 10 year mark
- Top Secret access: SSBI at 5 year mark
- Go back 5 years or to the last investigation date for all required information.

Back to Table of Contents
Index

Security Clearance Adjudications - Central Clearance Facility (CCF)

- For special assistance or advice, contact CCF Special Actions (DSN) 923-7613/2316 or (COML) (301) 677-7613/2316 or the CCF web page:
  - http://www.perscom.army.mil/gendocs/ccfpage.html

Back to Table of Contents
Index

Reporting Derogatory Information

Back to Table of Contents
Index

Definition

- **Derogatory Information-** Any information which reflects adversely on an individual's loyalty, trustworthiness, or sense of responsibility.

Back to Table of Contents
Index

Must a Commander Report Derogatory Information?

Back to Table of Contents
Index

Must a Commander Formally Suspend Access

- **No**
  - Submit DA Form 5248-R to CCF when reporting derogatory information
  - Only very serious incidents require formal suspension
  - Only CCF can restore access when it has been formally suspended

Back to Table of Contents
Index

Requesting Investigative File

- **Include in written request:**
  - Your full current name
  - Any other names used
  - Date of birth
  - Social security number
  - A notarized signature
  - A brief description of requested records
  - Any information you may believe useful in assisting in the record search
  - Whether or not you want someone else to receive the records for you (include name and address)

Back to Table of Contents
Index

Emergency Interim Security Clearance (EISC)

- EISC requirements pertain to recruiting U.S. civilian personnel in sensitive positions that require a security clearance
- Security Managers should establish a liaison officer with their local civilian personnel office to ensure security clearance requirements are met when U.S. civilians are appointed to sensitive positions

Back to Table of Contents
Index

Who Requests ANACI?

- It is the CPAC's responsibility to initiate the Access National Agency Check with written Inquiries (ANACI). This check is used for suitability determination for employment. However, the investigation is sufficient for Central Clearance Facility to grant a Secret or Confidential clearance.

Back to Table of Contents
Index

Who Can Grant an EISC?

- The Deputy Chief of Staff, Intelligence (AEAGB-CI-S) is the only approval authority

Back to Table of Contents
Index

Request for EISC's Will be Favorably Considered When:

- The requests are submitted in accordance with USAREUR Suppl 1 to AR 380-67 and
- There is no known derogatory information

Back to Table of Contents
Index

Information Systems Position Designated ADP-I, ADP-II, & ADP-III

- Security managers will keep a record identifying positions designated as ADP-sensitive. This record will consist of level of sensitivity of the position and the type of investigation required
- Foreign National (FN) personnel in sensitive ADP positions are subject to investigations

Back to Table of Contents
Index

ADP-I Positions

- A single scoped background investigation (SSBI) or a periodic reinvestigation (PR) is required regardless of date of hire. The DCSINT(AEAGB-CI-S) is the approving official.
  - ADP-1 for FNs: Investigation requests will be submitted following LAA procedures (USAREUR Suppl 1 to AR 380-67)
  - Access to classified information is not authorized for FNs
  - Persons occupying ADP-I positions are subject to the 5 year periodic reinvestigation (PR) requirement

Back to Table of Contents
Index

ADP-II & ADP-III Positions

- Foreign Nationals (FN's) will be screened as part of the hiring process IAW USAREUR Regulation 604-1, Foreign National Screening Program (Laredo Leader)

Back to Table of Contents
Index

Limited Access Authorization

- Limited Access Authorization (LAA) is a program for granting access to classified information to Foreign National employees.
- LAA’s are subject to a special background investigation every 5 years.

Back to Table of Contents

Index

LAA

- **Who can have access?**

- Foreign National (FN) employees who possess special skills or technical expertise that a U.S. citizen does not possess

- FN employees may be granted access to U.S. classified information that is determined releasable to the FN employee's country of citizenship

Back to Table of Contents

Index

LAA's

- LAA's will not be granted for single projects or for access to sites or restricted areas
- LAA holders are not authorized to act as couriers of classified information or leave the designated work area with classified information
- FN will not be given access to classified containers

Back to Table of Contents

Index

LAA's

- **How to request an LAA:**

  - Submit request to: HQ USAREUR & 7th Army ODCSINT, ATTN: AEAGB-CI-S, Unit 29351, APO AE 09014

  * Releasability determination
  * Commanders Statement, plus 2 copies
  * SF 86, plus 5 copies
  * AE Form 604-1A, plus 2 copies
  * Job description, plus 2 copies
  * Workplace diagram, plus 2 copies
  * 1879, plus 5 copies

Back to Table of Contents

Index

NATO Clearance for German Foreign Nationals (FN)

- Requests for NATO security clearances will be processed through the chain of command and sent to ODSCINT, ATTN: AEAGB-CI-S
- For German National USAREUR employees, the required paperwork will include a letter and three (3) copies of the German NATO clearance application
- The three (3) copies of the form must have original signatures
- The date of the signature must not be more than 60 days old when processed
- All blocks on form must be filled in

NATO Clearance for FNs (continued)

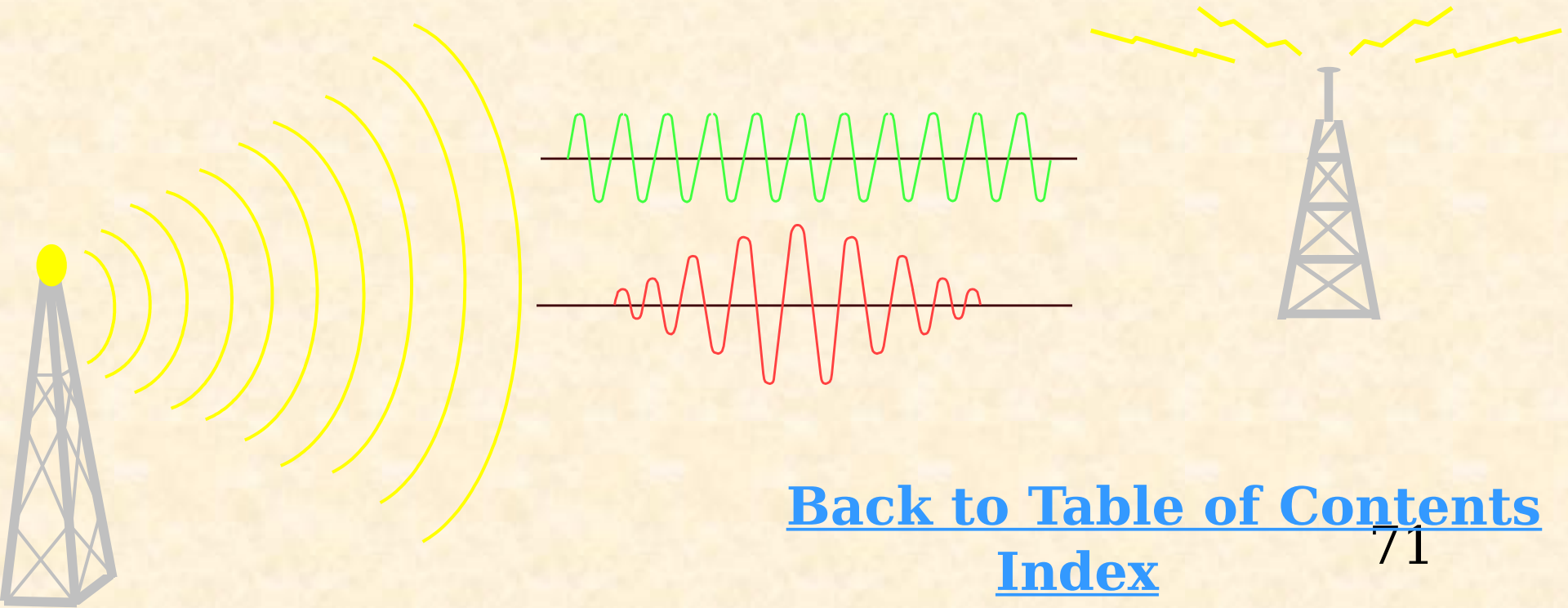
- A cover letter with
  - Name
  - DOB
  - Job title
  - Unit of assignment
  - Highest level of access required
  - Length of time the individual has worked for U.S. government
  - Full justification for requesting the clearance
  - Date and results of local files checks
- In order to obtain a NATO clearance, a FN must reside in his/her country of citizenship.

Back to Table of Contents

Index

Information Systems Security Monitoring

- **AR 380-53, 29 Apr 98**



Back to Table of Contents
Index

Discussion of Classified Information on the Phone

- Use a STU-III or some other authorized secure communication method
- Follow the encryption procedures for that piece of equipment
- Ensure that other people are not within hearing range of your voice

Back to Table of Contents
Index

What Can You Do?

- Avoid sensitive topics
- Know what you will say
- EEFI
- When in doubt go secure

Back to Table of Contents
Index

What Else Can You Do?

- Rule 1: Avoid talking about sensitive projects and missions over unsecured communications
- Rule 2: Know what you are going to say before you make a telephone call or get on a radio
- Rule 3: Pay attention to your Essential Elements of Friendly Information (EEFI) and avoid talking in the unsecured mode
- Rule 4: Remember Rule 1 and use secure communications when in doubt about the sensitivity of the subject to be discussed

Back to Table of Contents
Index

Where to Turn for Help?

- Assistance can be obtained from your supporting military intelligence (MI) unit. The supporting MI unit can provide a variety of services to help your unit identify problem areas and recommend corrective actions to counter your vulnerabilities

Back to Table of Contents

Index

USAREUR Communication Security Awareness Briefing:

- Do not discuss classified information on non-secured telephones. Official DoD telephones are subject to monitoring for information systems security at all times
- DoD telephones are provided for the transmission of official government information only and are subject to information systems security monitoring at all times. Use of official DoD telephones constitutes consent to information systems security telephone monitoring in accordance with DoD directive 4640.6. All other DoD telecommunication systems are likewise provided for the transmission of official government information only and are subject to information systems security monitoring at all times. Use of official DoD telecommunications systems constitutes consent to information systems security monitoring in accordance with DoD directive 4640.6

Information Systems Security
AR 380-19, 27 Feb 98

Back to Table of Contents
Index

Minimum INFOSEC Requirements

- All AIS will meet and maintain the following minimum requirements in order to operate:
  - System safeguards
  - Security and training awareness
  - Software/hardware controls
  - Procedures for marking removable magnetic media
  - Marking output at the appropriate level of classification
  - Least privilege: user access only to information they need
  - Safeguards for data integrity (safeguards to detect/prevent unauthorized access and malicious codes)
  - All AIS will be accredited

Back to Table of Contents
Index

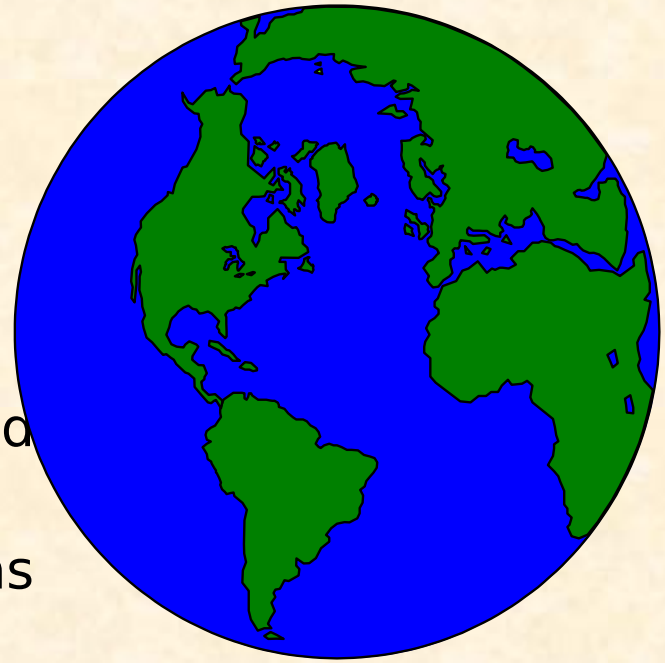
System Security Program/Safeguards

- A balanced information security program will include the following:
  - Good personnel security management/program
  - Safeguards to prevent unauthorized access to systems
    - Passwords
    - Limited access (buildings/ rooms locked after duty hours, computers not left while logged on)
  - Security incident reporting procedures are established
  - Security awareness program is in place
  - ISSM/ ISSO are appointed on orders and trained

Back to Table of Contents
Index

AIS Threat

- 126 countries have computer espionage programs
- Reported computer break-ins are expanding at over 52%
- DoD considered “easy pickings” by computer underground
- Computer crime recognized as fastest growing component of global organized crime
- Insiders pose a major threat to systems
- Malicious codes cause loss of information and time



Back to Table of Contents
Index

Types of Threats

Hackers

Insiders/Auth Users

Criminals & Organized Crime

Malicious Codes

Industry & Economic Espionage

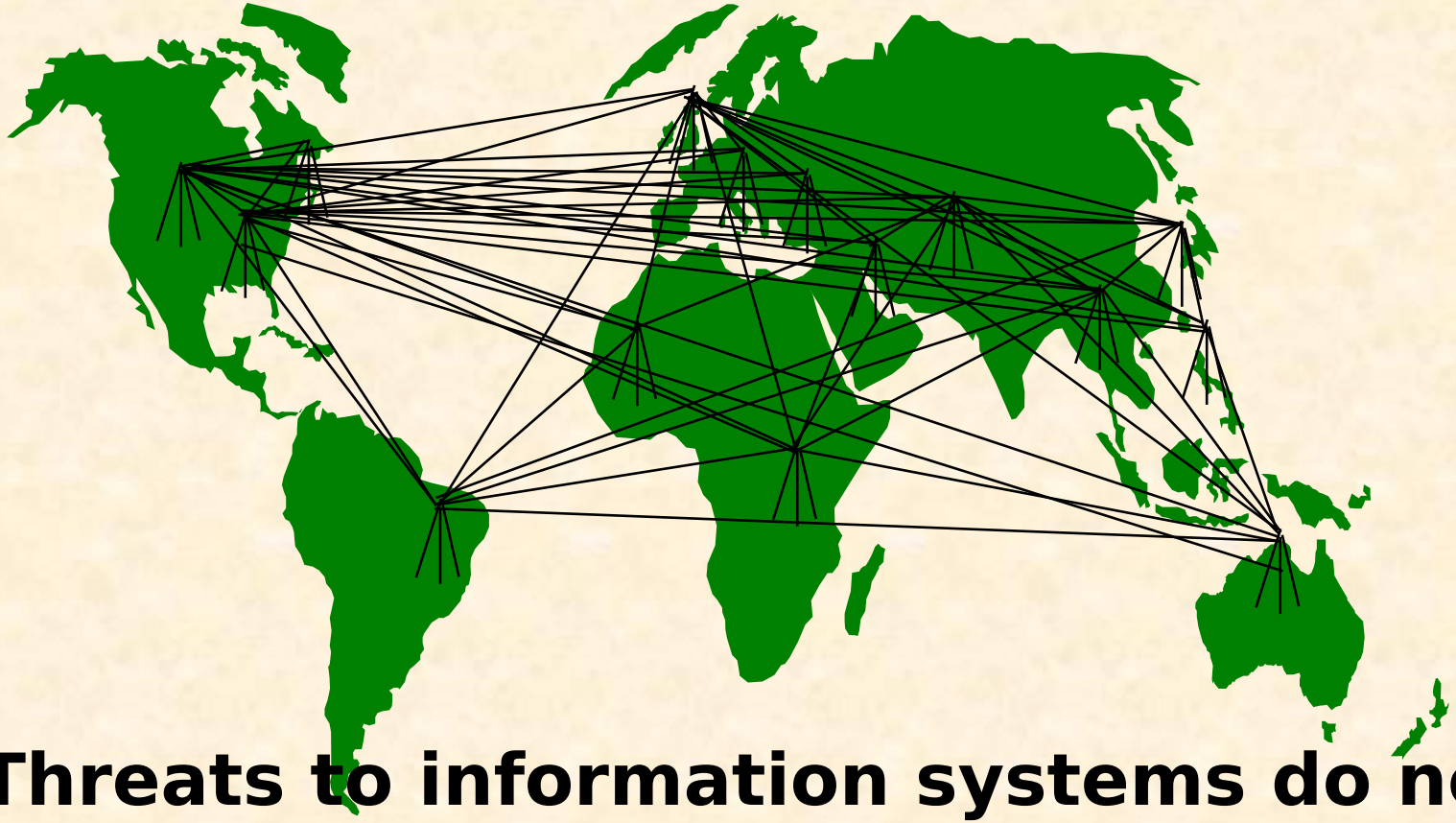
Foreign Countries

Terrorists

Index

Back to Table of Con

Information System Threat is Global



Threats to information systems do not recognize either physical or political boundaries.

Index Back to Table of Con

Where is the Threat?

- Foreign Intelligence Services
- Industrial Espionage
- Media
- Drug Smugglers
- Criminals
- Hobbyists

Back to Table of Contents
Index

What Type of Information Do We Disclose?

- Real work contingency operations
- Exercise information
- VIP itineraries
- Logistical information
- Communication architecture
- New systems
- Special operations

Back to Table of Contents
Index

Subversion and Espionage Directed Against the Army

AR 381-12, 15 JAN 93

UR 381-12, 27 SEP 90

CHANGE 1, 12 MAY 92

Back to Table of Contents

Index

What Types of Incidents Do You Report?

- Incidents of known, suspected, or possible espionage
- Suspicious questioning concerning military duties or required to provide military information
- Acts of deliberate compromise committed, attempted, or contemplated by DA personnel
- Contacts of DA personnel with known or suspected members of a foreign intelligence, military, or police agency
- Information concerning international terrorist activated or plans posing a direct threat to U.S. facilities or personnel

Back to Table of Contents
Index

Who Do You Report SAEDA Incidents To?

- DA & USAREUR policy requires you to report SAEDA incidents directly to your local MI detachment
- Knowledge of a SAEDA incident will be limited to as few persons as possible and only those who have a need-to-know. Do not tell commander, co-workers, friends, spouses, etc.

Back to Table of Contents
Index

USAREUR SAEDA Briefing

As a member of the U.S. Forces in Europe, you will have access to sensitive information, some classified. The U.S. Army Operations Security Program is designed to control and deny the enemy sensitive information. USAREUR and the Intelligence Community needs your help in this effort.

Back to Table of Content

Index

Operation Security - OPSEC

- AR 530-13
- Phone # (DSN) 370-6224/6168
- Proponent for OPSEC in USAREUR is DSCOPS

Back to Table of Contents

Index

Description

USAREUR Operations Security Program is designed to control and deny the enemy, sensitive information. All DA civilians and soldiers need to be briefed on their responsibilities in practicing good OPSEC.

Back to Table of Contents
Index

The following OPSEC elements require your special attention:

Back to Table of Contents
Index

Information Security 1

- Security to prevent disclosure of operation information by written, oral, or graphic communications
  - Protect, dispose of, and strip all maps as classified material, even strip maps or hand drawn maps of area
  - Use extreme caution when discussing field exercises, even with family members. Be careful with whom and where you discuss “going to the field”. The length and purpose of your absence and your field location could be critical information to the enemy

Back to Table of Content
Index

Signal Security -SIGSEC 2

- Security to prevent disclosure of information by telephone or radio
  - Do not discuss sensitive information over the telephone or an unsecured radio. Telephone and radio communications are monitored by unfriendly agents
  - Use secure voice telephone, AUTOSEVECOM, if available, for classified information. Classified electrically transmitted message channel should be used when secure voice is not available

Back to Table of Contents
Index

Physical Security 3

- Security to prevent or limit hostile individuals access to military facilities, equipment, material, documents, and VIP personnel
  - Note that most of USAREUR military installations are protected by fences or walls and normally have gate guards assigned at entrances
  - Proper identification is required to enter USAREUR military installations and restricted areas within installations

Back to Table of Contents
Index

You can prevent the enemy from gaining sensitive information when you practice good OPSEC. You are an important member of the USAREUR OPSEC team and we are counting on you to do your part.

Back to Table of Contents
Index

USAREUR TRAVEL POLICY

Back to Table of Content
Index

USAREUR Travel Policy

- The listings below will assist you in obtaining current travel advisory information via the internet:

http://www.state.gov

http://www.gsa.gov/travel.htm

http://travel.state.gov/travel_warnings.html

Back to Table of Contents

Index

USAREUR Travel Policy

- You can also listen to travel warnings (as well as consular information sheets with facts about various countries and public announcements) 24 hours a day by calling stateside: 202-647-5225 from a touch tone phone.
- Printed information may be obtained by sending a self-addressed, stamped envelope to:
  - Office of Overseas Citizens Services
  - Room 4800, Department of State
  - Washington, DC 20520-4818
  - Write the name of the requested country or countries on the outside of the envelope

Back to Table of Contents

Index

What are the Travel Warnings, Consular Information Sheets, & Public Announcements?

Back to Table of Contents

Index

Travel Warnings

- Travel warnings are issued when the State Department decides, based on all relevant information, to recommend that Americans avoid travel to a certain country. Countries where avoidance of travel is recommended will have travel warnings as well as consular information sheets.

Back to Table of Contents
Index

Public Announcements

- Public announcements are a means to disseminate information about terrorist threats and other relatively short-term and/or trans-national conditions posing significant risks to the security of American travelers. They are made any time there is a perceived threat and usually have Americans as a particular target group. In the past, public announcements have been issued to deal with short-term coups, bomb threats to airlines, violence by terrorists, and anniversary dates of specific terrorist events.

Back to Table of Contents
Index

Consular Information Sheets

- Consular information sheets are available for every country in the world. They include such information as location of the U.S. Embassy or Consulate in the subject country, unusual immigration practices, health conditions, minor political disturbances, unusual currency and entry regulations, crime and security information, and drug penalties. If an unstable condition exists in a country that is not severe enough to warrant a travel warning, a description of the condition(s) may be included under an optional section entitled “areas of instability.” On limited occasions, also restated in this section, any U.S. Embassy advice given to official employees. Consular information sheets generally do not include advice, but present information in a factual manner in order for the traveler to make his or her own decision concerning travel to a particular country.

Reporting Foreign Travel

- IAW DoD 5105.21-M-1, August 1998: All SCI indoctrinated personnel who plan official or unofficial foreign travel will report travel plans to local SCI security officials (SSO). (For personnel residing in a foreign country, foreign travel outside country of residence will be reported.)

Back to Table of Contents
Index

Foreign National Access to Installations in USAREUR

- USAREUR Suppl 1 to AR 380-67, 20 Jan 88
- Updated list of countries, Memo, 01 Apr 99

Back to Table of Contents
Index

Specified Country List

Afghanistan

Algeria

Burma

Cambodia

Cuba

Iran

Iraq

Former Yugoslavia (Serbia, Montenegro, and Bosnia Herzegovina)

Libya

Mongolia

North Korea

Peoples Republic of China (incl... Tibet)

Syria

Yemen

Back to Table of Contents
Index

Staff Assistance Visit (SAV)

Back to Table of Contents
Index

Staff Assistance Visits (SAV)

- Staff Assistance Visits (SAVs) will be conducted every other year or upon request. SAVs will be conducted by qualified security personnel and/or program managers to instruct security personnel and identify security program deficiencies.

Back to Table of Contents

Index

Index

- Accountability systems
- Allowing foreign national (FN) citizen passport holders access to installations in USAREUR:
- Communication security - COMSEC
- Consular information sheets
- DA & USAREUR policy requires you to report SAEDA incidents directly to you local MI detachment
- Definition
- Discussion of classified on the phone
- Emergency interim security clearance (EISC)
- End of the day security check
- Faxing classified information

Back to Table of Conte

Index

- Handcarrying
- Handling classified when not in a container
- Handling of mail
- How to mark documents on disk
- How to prepare classified for movement
- How to destroy
- How to mark disks
- Information security
- Initial investigations
- Knowledge of a SAEDA incident
- Methods for mailing classified documents
- Methods for transmitting classified materials

Back to Table of Con

Index

- Minimum marking requirements for paper products
- Must a commander formally suspend access?
- Must a commander report derogatory information?
- NATO clearance for German foreign nationals (FN)
- Operation security - OPSEC
- Periodic reinvestigations
- Physical security
- Procedures to follow when reproducing classified
- Public announcements
- Reporting derogatory information
- Request for EISC’s
- Requesting investigative file

Back to Table of Conte

Index

- Security clearance adjudications - Central Clearance Facility (CCF)
- Security clearance investigative requirements
- Signal security -SIGSEC
- Specified-country passport holders not allowed on USAREUR installations list
- Subversion and espionage directed against the army
- Transporting from office to office
- Travel warnings
- USAREUR installation that have controlled access due to force protection measures, must adhere to the following:
- USAREUR limited access authorization (LAA)

Back to Table of Contents

Index

- USAREUR travel policy
- Using distribution systems
- Using your security container
- What types of information do we disclose?
- Where is the threat?
- Where to turn for help?
- Who approves LAA’s?
- Who can destroy classified materials?
- Who can grant an EISC?
- Who can have access?
- Who is eligible for an LAA?

Back to Table of Content

Index

- Who needs to report travel?
- Who requests NACI?
- What can you do?
- What else can you do?
- What to destroy?
- What to do when no one is in the office to receive mail?
- What to do while distributing classified?
- What to do with the disk?
- What to do with the drafts/notes/etc…?
- What to do with the materials while typing?
- What to do with the typewriter/printer ribbon?

Back to Table of Contents